PURPOSE

This transmits new text for IRM 1.16, Section 1, Physical Security Program, which replaces text 1(16)10 and 11 of IRM 1(16)00, Physical, Document and Computer Systems Security Manual.

BACKGROUND

The IRM is being converted to a new format and style which will be issued in 8½" x 11" instead of the current 6" x 9" size. The new IRM includes simplified text, a new numbering system, and a new format for organizing text.

The IRM text pertaining to the purpose authority, directives, and reponsibilities has been reorganized and renumbered. This transmittal reissues existing information in the new IRM format. It replaces text currently contained in IRM 1(16)10 and 11, which are being obsoleted.

NATURE OF MATERIALS

This new IRM 1.16, Physical Security program, provides an overview of the physical security program within the IRS, as well as the legal authority for the program.

Leland N. Keller
National Director, Real Estate
Planning and Management Division

Table of Contents

1.1 (02/16/99)
Purpose

(1) The Internal Revenue Service processes sensitive data, such as

- private information of U.S. citizens
- financial information,
- law enforcement information,
- proprietory information, and
- life and mission-critical information.

(2) Inadvertent or deliberate disclosure, alteration or destruction of this sensitive data pose such risk and high degree of harm that the Service must protect its information resources through

- physical security,
- data security, and
- other security procedures.

(3) Security procedures must also allow for access, use, disclosure and disposition of information in strict accordance with applicable laws, federal regulations, and Treasury Department directives.

(4) Service officials and managers are responsible for the secure operation of the federal tax administration system and for taking actions sufficient to prevent loss of life and property, disruption of services and functions, and unauthorized disclosure of documents and information.

1.2 (02/16/99)
Authorities

1. Executive Order 12356, National Security Information
2. The Privacy Act of 1974
3. Tax Reform Act of 1976
4. IRC 6103, 7213, 7217, and 7431
5. Federal Managers' Financial Integrity Act of 1982 (FMFIA)
6. Government Accounting Office Standards
7. OMB Circular A–123 (Internal Control System)
8. OMB Circular A–130 (Security of Federal Automated Systems)
9. Treasury Security Manual 71–10

1.3 (02/16/99)
Directive

(1) Overriding principles of security in the Internal Revenue Service:

- Every employee is responsible for security;
- Access to sensitive information should be granted only on a need-to-know basis;
- Managers and employees are responsible for providing reasonable security for all information, documents, and property entrusted to them.

(2) Established guidelines for minimum security standards allow flexibility to develop higher standards when needed to meet local situations. These guidelines can be found in the Physical Security Handbook and encompass

- security reviews,
- crisis management,
- ID media,
- document security, and
- minimum standards for safeguarding personnel, facilities, and property.

1.4 (02/16/99)
Responsibilities

(1) The **Chief, Management and Finance** has overall responsibility for the Servicewide Physical Security Program.

(2) The **National Director, Real Estate Planning and Management Division**, is responsible for developing, monitoring, evaluating, and managing the Servicewide Physical Security Program.

(3) Each **Regional Commissioner** must maintain an effective regional physical security program.

(4) Each **District Director, Service Center Director, Atlanta Customer Service Center Director, Regional Counsel, National Office Division Director**, and **Computing Center Director** is responsible for an effective physical security program and reasonable and adequate security measures.

(5) The **National Office Director of Support and Services** plans and evaluates the program for National Office and makes sure that security measures meet established minimum security standards.

(6) **Directors of Support Services** make sure that **Host Site Chiefs** are in compliance with Service policy and provide guidance, oversight, and help to host sites and client sites with the physical security program.

(7) **Host Site Chiefs** plan, develop, and evaluate physical security programs for their host and client sites, making sure that Service policy and procedures are followed and that security measures meet established minimum security standards.